

[Newsroom](#) [Site Map](#) [Contact NERC](#)**Comment Form: Project 2008-06 Version 5 CIP Standards (Phase III)**

IMPORTANT NOTE: *Please make sure to hit the FINISH button at the bottom of this screen to submit your comments to NERC. A verification code will be provided on the next screen.

Survey Response: Comment Form: Project 2008-06 Version 5 CIP Standards (Phase III)

Comment Request - Project 2008-06 Version 5 CIP Standards (Phase III)

Response GUID: 24a7df67-be8f-4f76-acb7-51172b30193a

Started: 1/6/2012 4:59:07 PM

Completed: 1/6/2012 5:18:05 PM

Page 2

1) **Individual or group.**

Group

Page 4

2) **Group Name**

Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)

3) **Lead Contact**

Marianne Swanson

4) **Contact Organization**

National Institute of Standards and Technology (NIST)

5) **Registered Ballot body segment (check all applicable industry segments)**

9 - Federal, State, Provincial Regulatory, or other Government Entities

6) **Contact Telephone**

###-###-####

301-975-3293

7) **Contact E-mail**

marianne.swanson@nist.gov

8) **Please complete the following information.**

	Additional Member	Additional Organization	Region	Segment Selection
1.	Victoria Yan Pillitteri	Booz Allen Hamilton	NA - Not Applicable	NA
2.	David Dalva	Booz Allen Hamilton	NA - Not Applicable	NA

- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.
- 11.
- 12.
- 13.
- 14.
- 15.
- 16.
- 17.
- 18.
- 19.
- 20.
- 21.
- 22.
- 23.
- 24.
- 25.

Page 5

9) **Question 1**

1. Many definitions in the Definitions document contain modified definitions from existing terms and new definitions for terms used in these standards. Do you have any suggestions that would improve the proposed definitions? If so, please explain and provide specific suggestions for improvement.

No

Page 6

10) **Question 2**

2. CIP-002-5 Attachment 1 contains criteria that provide the basis for the categorization of BES Cyber Systems and BES Cyber Assets. Most of these criteria are similar to those already approved by the industry as part of Version 4. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

Yes

11) **Question 2 Comments:**

The Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has developed a mapping between NERC CIP v5 requirements and the high-level security requirements in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Security. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

This mapping identifies any gaps between CIP v5 and the NISTIR 7628 high-level security requirements and recommendations to the CIP drafting team to consider.

The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were identified.

The CIP-002-5 criteria provide a sound approach for identifying low, medium, and high impact systems within the BES. This three level approach aligns well with the three level approach (i.e., low, moderate, and high) used within the NISTIR. Most requirements in the current CIP drafts are applicable to both medium and high impact systems as a bundled pair and they are silent on their applicability to low impact systems. In contrast, the NISTIR uses a graded requirement approach that specifies baseline controls that apply at low impact levels and then specifies strengthened controls for moderate impact and even stronger controls for high impact levels. The CIP version 5 standards will be significantly strengthened if they were to incorporate a similar graded approach when applying requirements.

Page 7

12) Question 3

3. Requirement R1 of draft CIP-002-5 states, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

No

13) Question 3 Comments:

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R1, 1.1, to include the concept of "continuous improvement" and best practices (to align to NISTIR 7628, SG.CA-3, Continuous Improvement).

Page 8

14) Question 4

4. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

Yes

Page 9

15) Question 5

5. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 10

16) **Question 6**

6. CIP-003-5 R1 states "Each Responsible Entity shall identify, by name, a CIP Senior Manager." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

Yes

Page 11

17) **Question 7**

7. CIP-003-5 R2 states "Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

No

18) **Question 7 Comments:**

To align with the NISTIR 7628 high-level requirements, CIP should elaborate requirement:

R2, 1.3, to include following -

1) Responsible Entity should document document allowed methods of access to the BES Cyber Systems (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures);

2) Responsible Entity should incorporate in their policies the usage restrictions and criteria for allowing each remote access (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures);

3) Responsible Entity should setup authorization procedures prior to granting remote access;

4) Responsible Entity should enforce requirement criteria for providing remote access to the BES Cyber systems (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures);

5) Responsible Entities shall implement policies and procedures for managing remote sessions in their BES Cyber Systems access control policies and procedures (to align with NISTIR 7628, SG.AC-13, Remote Session Termination);

6) Responsible Entities shall include in procedures and criteria of granting Remote access encryption, authentication of all communication media through limited number of manageable access control points (to align with NISTIR 7628, SG.AC-15, Remote Access).

R2, 1.5 to include following -

Responsible Entities shall include in their policies and procedures to grant access privileges to their BES information Systems based on minimum privilege justified by the business requirement for access requests (to align with NISTIR 7628, SG.AC-19, Control System Access Restrictions).

R2, 1.6 to include details on what the policy should address including objectives, roles and responsibilities, and the the scope of the incident response program, and require the identification and classification of potential interruptions (to align with NISTIR 7628, SG.IR-1, Incident Response Policy and Procedures).

R2, 1.7 to specify required elements of the recovery plan (to align with NISTIR 7628, SG.CP-1, Continuity of Operations Policy and Procedures and SG.CP-2, Continuity of Operations Plan).

R2, 1.9 to include following -

- 1) Responsible entities shall restrict access to external information systems or restrict processing, storing or transmitting controlled information through External Information systems over which the Responsible Entities have no control (to align with NISTIR 7628, SG.AC-18, Use of External Information Control Systems);
- 2) Responsible entities shall have a documented media protection security policy that addresses the objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization's personnel and assets; the scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and procedures to address the implementation of the media protection security policy and associated media protection requirements (to align with NISTIR 7628, SG.MP-1, Media Protection Policy and Procedures); and
- 3) Requirement that data communications be addressed in the information protection policy (to align with NISTIR 7628, SG.SC-1, System and Communication Protection Policy and Procedures).

Page 12

19) **Question 8**

8. CIP-003-5 R3 states "Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

Yes

Page 13

20) **Question 9**

9. CIP-003-5 R4 states "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." Do you agree with the proposed Requirement R4? If not, please explain why and provide specific suggestions for improvement.

Yes

Page 14

21) **Question 10**

10. CIP-003-5 R5 states "The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated." Do you agree with the proposed Requirement R5? If not, please explain why and provide specific suggestions for improvement.

Yes

Page 15

22) **Question 11**

11. CIP-003-5 R6 states "Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific

suggestions for improvement.

Yes

Page 16

23) **Question 12**

12. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 17

24) **Question 13**

13. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 18

25) **Question 14**

14. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 19

26) **Question 15**

15. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 20

27) **Question 16**

16. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

28) Question 16 Comments:

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R4, 4.1, to include detailed personnel screening requirement detailed in NISTIR 7628, SG.PS-3, Personnel Screening, as follows:

Basic screening requirements should include -

- a. Employment history;
- b. Verification of the highest education degree received;
- c. Residency;
- d. References; and
- e. Law enforcement records.

Page 21

29) Question 17

17. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 22

30) Question 18

18. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

31) Question 18 Comments:

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R6, 6.1, 6.2, 6.3, and 6.4 to include security authorization for granting escorted/unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management (to align with NISTIR 7628, SG.PS-7, Contractor and Third-Party Personnel Security).

R6, 6.5 and 6.6, to include security authorization for periodic review of permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management (to align with NISTIR 7628, SG.PS-7, Contractor and Third-Party Personnel Security).

Page 23

32) **Question 19**

19. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

33) **Question 19 Comments:**

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R7, 7.1, to include requirement of exit interview to convey the constraints imposed on the individuals/ contractors/ Third Party Service Providers, due to revocation of privileges caused by change in assignments or termination of job (to align with NISTIR 7628, SG.PS-4, Personnel Termination).

Page 24

34) **Question 20**

20. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 25

35) **Question 21**

21. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

36) **Question 21 Comments:**

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R1, 1.2, to identify -

1) specific authentication credential management requirements (initial authentication credential content; administrative procedures for initial authentication credential distribution/lost credentials/lost, compromised, or damaged authentication credentials/revoking authentication credentials; changing/refreshing authentication credentials on an organization-defined frequency; and specifying measures to safeguard authentication credentials) (to align with NISTIR 7628, SG.IA-3, Authenticator Management); and

2) devices to be identified and authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication).

R1, 1.3 to identify devices to be identified and authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication).

Page 26

37) **Question 22**

22. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

38) **Question 22 Comments:**

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R2, 2.1, to include -

1) The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications;

2) The organization changes the diversity of operating systems and applications on an organization-defined frequency; and

3) The organization employs randomness in the implementation of the virtualization (to align with NISTIR 7628, SG.SC-28, Virtualization Technique).

R2, 2.2, to include -

1) cryptographic key establishment and management (to align with NISTIR 7628, SG.SC-11, Cryptographic Key Establishment and Management); and

2) use of FIPS-140-2 approved or allowed cryptography and other security functions (to align with NISTIR 7628, SG.SC-12, Use of Validated Cryptography).

Page 27

39) **Question 23**

23. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 28

40) **Question 24**

24. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 29

41) **Question 25**

25. CIP-006-5 R2 states "Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and

its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 30

42) **Question 26**

26. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 31

43) **Question 27**

27. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 32

44) **Question 28**

28. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 33

45) **Question 29**

29. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 34

46) **Question 30**

30. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 35

47) **Question 31**

31. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

48) **Question 31 Comments:**

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R4, 4.2, to specify -

1) the use of an automated mechanism to necessitate a real-time alert (to align with NISTIR 7628, SG.IR-6, Incident Monitoring); and

2) receiving security alerts, advisories, and directives from external organizations (to align with NISTIR 7628, SG.SI-5, Security Alerts and Advisories).

R4, 4.3, to specify some events that alerts should be generated (to align with NISTIR 7628, SG.AU-5, Response to Audit Processing Failures).

Page 36

49) **Question 32**

32. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

50) **Question 32 Comments:**

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R5, 5.1 to specify devices to be identified/authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication).

R5, 5.3 to specify requirements for managing authentication credentials for users/devices, including supplemental guidance to safeguard credentials by not loaning/sharing credentials (each individual must be identified for any shared account as opposed to sharing credentials) (to align with NISTIR 7628, SG.IA-3, Authenticator Management).

Page 37

51) **Question 33**

33. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 38

52) **Question 34**

34. CIP-008-5 R1 states "Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

53) **Question 34 Comments:**

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R1, 1.3, to specify -

1) data is reported in compliance with applicable laws and regulations (to align with NISTIR 7628, SG.IR-7, Incident Reporting);

2) external entities that should be considered for not only communication but coordinated effort related to cyber security incidents (to align with NISTIR 7628, SG.IR-11, Coordination of Emergency Response).

Page 39

54) **Question 35**

35. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 –BES Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

55) **Question 35 Comments:**

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R2, 2.1, to specify the use of an automated mechanism in response to an incident (to align with NISTIR 7628, SG.IR-6, Incident Monitoring).

Page 40

56) **Question 36**

36. CIP-008-5 R3 states "Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 41

57) **Question 37**

37. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 42

58) Question 38

38. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

59) Question 38 Comments:

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R1, 1.3, to specify information to be backed up (to align with NISTIR 7628, SG.IR-10, Smart Grid Information System Backup). Information to be backed up includes user-level information, system-level information and system documentation including security related documentation. The confidentiality and integrity of the backup information shall be maintained.

R1, 1.3, 1.4, and 1.5 to specify alternate storage sites (to align with NISTIR 7628, SG.CP-7, Alternate Storage Sites) and requirements to recover/reconstitute Smart Grid systems to a secure state (to align with NISTIR 7628, SG.CP-10, Smart Grid Information System Recovery and Reconstitution).

Page 43

60) Question 39

39. CIP-009-5 R2 states "Each Responsible Entity shall implement one or more processes that collectively address the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

61) Question 39 Comments:

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R2, 2.1, 2.2, and 2.3, to specify requirements to recover/reconstitute systems to a secure state (to align with NISTIR 7628, SG.CP-10, Smart Grid Information System Recovery and Reconstitution).

Page 44

62) Question 40

40. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 45

63) Question 41

41. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 46

64) Question 42

42. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 47

65) Question 43

43. CIP010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 48

66) Question 44

44. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 49

67) Question 45

45. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 50

68) Question 46

46. CIP-011-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-5 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

No

69) **Question 46 Comments:**

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement:

R1, 1.1 to specify -

1) requirements to partition the communications for telemetry/data acquisition services and management functionality. The information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path (to align with NISTIR 7628, SG.SC-2, Communications Partitioning); and

2) requirements to employ underlying hardware separation mechanisms to facilitate security function isolation; and isolate security functions (e.g., functions enforcing access and information flow control) from both non-security functions and from other security functions (to align with NISTIR 7628, SG.SC-3, Security Function Isolation).

R1, 1.2 to specify more granular retention requirements as applicable to law/regulations (to align with NISTIR 7628, SG.IA-2, Identifier Management).

Page 51

70) **Question 47**

47. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-5 Table R2 – Media Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

Page 52

71) **Question 48**

48. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

Page 53

72) **Question 49**

49. Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement.

Yes

<< Back

Save and Quit

Finish